THE OFFICE OF THE LEGAL SERVICES COMMISSIONER

CLOUD COMPUTING PRACTICE NOTE

The term “cloud computing” is commonly used to refer to the delivery of hosted services over the Internet. These services are offered from data centers all over the world and are collectively referred to as the ‘cloud’. Any user with an Internet connection can access the cloud and the services it provides. Cloud computing is simply a way to describe how individuals and organizations can take some or all of their existing IT data infrastructure and operations and hand it over to a third party to build or manage.

The use of cloud computing is particularly common for communication services such as email (e.g. gmail/hotmail) and is becoming increasingly common in legal practices. Cloud computing offers a legal practice the opportunity to access and pay for services as they are used, rather than the legal practice having to maintain its own software support resources.

In some cases, law practices may not always be aware that business and client records may already be in the cloud, as domestic internet service providers purchase wholesale services including cloud technology and services that are on sold to domestic retail clients.

Whilst cloud computing can provide lawyers with new opportunities to conduct their practice, the services offered can compromise a lawyer’s professional and ethical obligations if not implemented carefully. Cloud computing service providers often hold data and operate servers overseas, sometimes in varying locations depending on cost, resource availability and time zone requirements. Breaches of confidentiality and security, for example, can occur where client information is stored by third parties in the cloud computing environment.

This practice note is designed to assist by setting out guidance for lawyers when using cloud computing services in their legal practice.

This practice note should be considered in light of the legislation, Rules and common law. The practice note is intended to be read in conjunction with the relevant practice rules and statements of ethics in the *Legal Profession Uniform Law (NSW) 2014*, the *Legal Profession Regulation* and the *Solicitors’ Rules*. Since the practice note is not part of the Solicitors Rules its contents are not binding.

Practice Note

The Solicitors’ Rules apply to lawyers practising as solicitors or as barristers and solicitors, including those who use cloud computing services in their legal practice.

Lawyers cannot contract out of their professional obligations owed to the Court or their client or delegate them to another person.

Rules dealing with Competence and diligence, Confidentiality and File Retention are particularly relevant to the use of cloud computing services by lawyers.

A lawyer's fiduciary obligations to their client inherently require maintenance of confidentiality of client information unless otherwise authorized.

A lawyer must obtain consent from their client before disclosing the client's confidential information to a person other than a principal or employee of the legal practice, or another person to whom disclosure is authorized by law, such as an auditor or professional indemnity insurer.

A lawyer is responsible for retaining, securely and confidentially, documents prepared under their retainer for their client or received from third parties.

Lawyers who use cloud computing services are responsible for supervising the legal services provided to the client, including those impacted by work or services located or accessed through the cloud.

Contemplation: When contemplating using cloud computing services in their legal practice a lawyer should:

1. Obtain an appropriate understanding of cloud computing technology;

2. Consider whether use of cloud computing services will benefit the lawyer's clients;

3. Consider whether the use of cloud computing services will benefit the lawyer's practice;

4. Ensure they are able to comply with their professional/ethical obligations;

5. Appreciate and appropriately manage the risks that may arise with the use of cloud computing services.

Client consent: The use of a cloud computing service provider may result in the disclosure of client confidential information.

It may be that either no client confidential information will be transferred to the cloud computing service provider, or if such information is transferred and stored with the cloud computing service provider the provider and its staff are not able or will not access that information such that the client confidential information cannot be said to be disclosed to the cloud computing service provider.

Prior to using cloud computing services in their legal practice where client confidential information will be disclosed to the cloud computing service provider a lawyer should obtain informed consent from any client whose confidential information may be disclosed.

As client authorization is needed to disclose client information to cloud computing service providers, a lawyer should either obtain such consent specifically from the client or consider including clauses in their standard retainers.

Due diligence: Prior to using cloud computing services in their legal practice a lawyer should undertake appropriate due diligence on the proposed cloud computing service provider/s including consideration of the following:

1. Whether the cloud computing service provider meets required standards of competency;

2. What security the cloud computing service provider has in place to maintain confidentiality of confidential information of the lawyer's client and reduce risks of unauthorized access, inadvertent disclosure and reckless or intentional compromise by employees;

3. The extent to which the following may impact a lawyer's ability to comply with their professional obligations:

   (a) The supervisory regime (if any) applicable to the cloud provider; and

   (b) The laws applicable in that jurisdiction to privacy and security. Some jurisdictions (eg the USA Patriot Act) enable access to client information that would otherwise remain confidential. Also, jurisdictions that don't have a comparable privacy regime to Australia may require enhanced contractual obligations to ensure the cloud computing provider abides by the same obligations applicable in Australia.

The cloud computing service arrangement: Cloud providers will generally have standard form terms and conditions that apply to all their customers. When entering into a contract with a cloud computing service provider a lawyer should consider the following issues:

1. A contractual obligation that the outsource provider conduct its services or activities in a manner that does not cause the lawyer to breach their professional obligations;

2. The choice of law to govern the contractual obligations;

3. The jurisdiction in which any client confidential information will be held;

4. The manner in which the cloud computing service provider holds and deals with client confidential information;

5. The security framework in place offered by the outsourcer as well as information about storage and back up security;

6. Whether the cloud computing service provider contractually undertakes to keep the information confidential and to procure its staff to keep the information confidential;

7. The circumstances in which the cloud computing service provider's staff are authorized to access the confidential information of the lawyer's client;

8. The obligation to provide regular reports to the lawyer on its compliance with its contractual obligations and whether it must immediately report any breach or potential breach of those contractual obligations;

9. The provisions for protection of confidential client information from unauthorized access and inadvertent disclosure including for example:

    i. Encryption of data transferred on-line to external servers where the client's system also provide for such functionality;

    ii. Use of secure usernames and passwords;

    iii. Ensuring the cloud computing service provider has policies and procedures for privacy, and to protect confidential client information from unauthorized access and inadvertent disclosure.

10. Access the client confidential information held by the cloud computing service provider at any time and particularly if the cloud computing service provider becomes financially distressed, defunct or suffers a disaster event;

11. The prescribed processes and timing for transition back to the lawyer from the cloud computing service provider or their successor of client confidential information on cessation of the arrangement (i.e. where the provider goes out of business or is taken over by another provider);

    (a) That the cloud computing arrangement is not used to put documents or evidence beyond the reach of the Courts.

12. The policies and procedures of the cloud computing service provider in relation to data preservation and destruction.

Practice management: When using cloud computing services it would be prudent for a lawyer to:

1. Put in place a Policy on Use of Cloud Computing Services to document appropriate requirements for the use of cloud computing services to the lawyer's practice;

2. Keep up to date on technological changes as they impact the lawyer's practice of law;

3. Keep up to date on the security issues related to the use of the technology chosen for the law firm. Designate a lawyer who is responsible for this task or retain the services of an IT consultant familiar with implementing cloud solutions in a law firm environment;

4. Have procedures and systems to ensure the lawyer's staff and other resources (including non-legal staff and outsource provided staff) are

competent in their understanding and use of cloud computing services in the lawyer's legal practice, use those cloud computing services appropriately and are appropriately supervised;

5. Take care with access settings for staff of the lawyer's legal practice to ensure cloud computing services are only available to appropriate contacts and that inadvertent access or disclosure of confidential client information cannot occur;

6. Never write down usernames and passwords for access to any cloud computing application. Make sure that the passwords you create are strong and change them regularly. If you have a number of passwords, use an application like `KeePass' to organize them all;

7. Ensure communications with clients through cloud computing service providers are clear and communication benefits do not suffer adversely through change of medium;

8. Maintain management of client expectation through advice on matter developments, explanation of legal processes and outcomes as you would through communications provided by more traditional medium;

9. Prepare an exit strategy that includes the full retrieval of all data;

10. Review and assess the information stored in the cloud in relation to retrieval, data integrity and compatibility;

11. Lawyers using cloud computing applications on mobile devices, might also follow these basic security tips:

    - If you use wireless networking, ensure that all wireless traffic is encrypted with WPA2.

    - Keep antivirus software and all software patches updated. Turn on the software firewall for the computer.

    - Use a safer browser with the No Script add-on installed, or use another pop-up blocker.

    - Avoid free Wi-Fi hotspots when using any cloud computing application remotely. Use a mobile phone modem adapter instead.